Sur le délai de séparabilité dans des systèmes synchrones

Ilias Garnier, Christophe Aussagès, Vincent David, Guy Vidal-Naquet

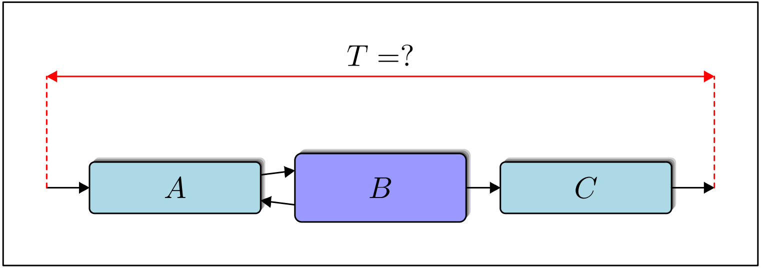
November 16, 2011

Plan

- Contexte
- Modèle formel
- Délai de séparabilité
- (Non)-compositionnalité
- Perspectives

Contexte et motivation

Systèmes temps-réels embarqués : systèmes informatisés intéragissant avec le monde physique sous contraintes temporelles fortes. Systèmes multi-tâches : contraintes de **bout-en-bout**.



Contexte et motivation - 2

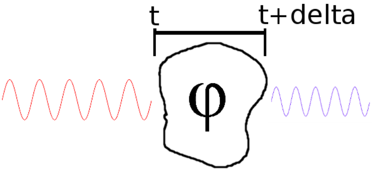
Méthode classique de modélisation de contraintes temporelles

Mesure de l'intervalle temporel entre évenements *symbolisant* observation et réponse du système.

Exemples :

- dates de mise à jour des flots d'entrée et de sortie du système (e.g. T. Le Berre 2010)
- analyses WCET

Existe-t-il une notion plus générale ? Analogie :



Idée : étude des dépendances fonctionnelles entre entrées et sorties

Plan de notre étude

- Machines de Moore
- Que signifie *réagir* à une entrée ?
  - existence d'un "effet observable"
  - $\Rightarrow$ besoin d'une notion formelle *d'équivalence observationnelle*
- Quelle notion de *délai* ?
  - dans notre cas, nombre de transitions jusqu'à un effet observable
- Pour les systèmes temps-réels répartis, besoin d'une notion de composition.
  - étude du délai de séparabilité sous composition séquentielle

Cadre d'étude

Cadre de notre étude : systèmes OASIS $\approx$ modèle synchrone faible. Etape de calcul dans le modèle synchrone faible :

$$
\begin{array}{ccccccc}
 & \text{time } t & & & & \text{time } t+1 & \\
Input_t & & Internal_t & & Input_{t+1} & & Internal_{t+1} \\
 & & & \Longrightarrow & & & & \dots \\
 & \Downarrow \text{reaction} & & & & \Downarrow \text{reaction} & \\
 & Output_t & & & & Output_{t+1} &
\end{array}
$$

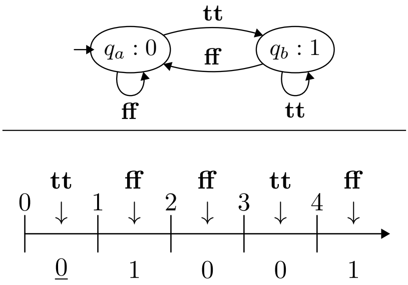
Calcul synchrone faible = séquence potentiellement infinie d'étapes de calcul. Quand l'espace d'état est fini, obtention d'une machine de Moore.

Machines de Moore

Machine de Moore = automate où les états sont étiquetés par les sorties. Soit **In** alphabet d'entrée, **Out** alphabet de sortie, $\mathcal{M} = \langle \mathbf{In}, \mathbf{Out}, Q, E, \mathbf{out} \rangle$.

- Q ensemble fini d'états,
- $E \subseteq Q \times \mathbf{In} \times Q$ ensemble d'arcs, *condition de totalité*
- $\mathbf{out} : Q \rightarrow \mathbf{Out}$ sorties.

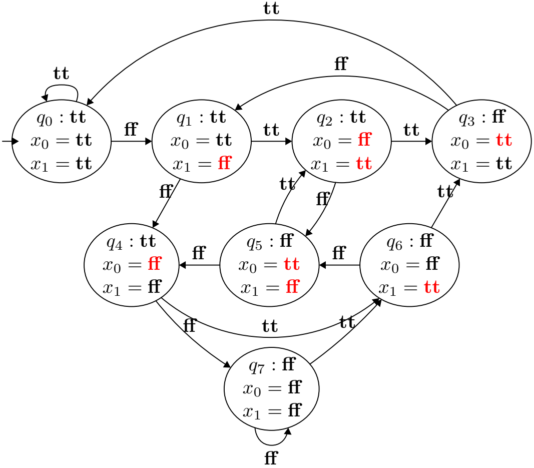
Petit exemple : sortie 0 si **ff**, sortie 1 si **tt**:



Autre exemple

Un programme synchrone et la machine associée :

x_0 := **true**;
x_1 := **true**;
while true do
  next(x_0);
  x_0 := x_1;
  x_1 := **input**
done



Equivalence observationnelle

Afin de définir ce qu'est un effet observable, nous avons besoin de définir l'équivalence observationnelle. Choix de la bisimilarité. Soient p et q deux états :

$$
\begin{array}{rcl}
p \sim q & \Leftrightarrow & \mathbf{out}(p) = \mathbf{out}(q) \wedge \\
& & \forall a, \forall p', p \xrightarrow{a} p' \Rightarrow \exists q', q \xrightarrow{a} q' \wedge p' \sim q' \wedge \\
& & \forall a, \forall q', q \xrightarrow{a} q' \Rightarrow \exists p', p \xrightarrow{a} p' \wedge p' \sim q'
\end{array}
$$

Intuitivement: $p \sim q$ est l'égalité des **dépliages** depuis p et q.

Délai de séparabilité - cas des fonctions totales

Délai de séparabilité $\approx$ délai entre entrée et sortie **fonctionnellement dépendante**.

$f : In \rightarrow Out$ une fonction totale. Nous avons :

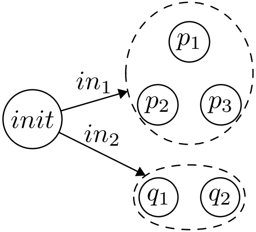
$$f \text{ constante} \Leftrightarrow f(In) = \{o\}$$

$$f \text{ non-constante} \Leftrightarrow \exists in_1, in_2, in_1 \neq in_2 \wedge f(in_1) \neq f(in_2)$$

(in_1, in_2) permet de prouver f non-constante : **paire séparante**.

Délai de séparabilité : cas des machines de Moore

état = fonction des entrées vers ensembles d'états



ensembles d'états atteignables P et Q non équivalents si $P/\sim \;\neq\; Q/\sim$.

Délai de séparabilité

Nombre de transitions pour <u>observer</u> que $P/\sim \;\neq\; Q/\sim$.

Effets observables

Effets observables extraits de contres-exemples à la bisimilarité.
Définition inductive de $p \not\sim q$:

$$\text{BASE}\ \frac{\mathbf{out}(p) \neq \mathbf{out}(q)}{p \not\sim q}$$

$$\text{IND}\ \frac{\forall a, \exists p', p \xrightarrow{a} p' \wedge (\forall q', q \xrightarrow{a} q' \Rightarrow p' \not\sim q')}{p \not\sim q} \qquad \text{SYM}\ \frac{q \not\sim p}{p \not\sim q}$$

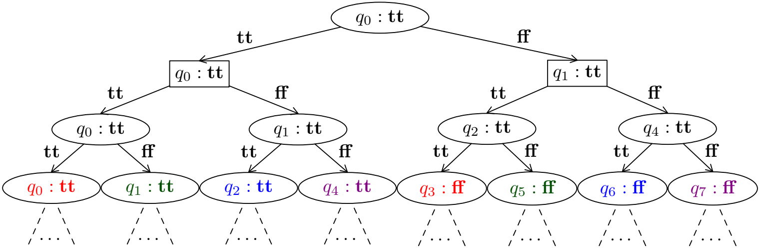
$$\left.\begin{array}{l} p = p_0 \xrightarrow{a_0} p_1 \xrightarrow{a_1} p_2 \dots p_n \\ q = q_0 \xrightarrow{a_0} q_1 \xrightarrow{a_1} q_2 \dots q_n \end{array}\right| \text{ s.t. } \mathbf{out}(p_n) \neq \mathbf{out}(q_n).$$

Effet observable, séparateur

La paire $(\mathbf{out}(p_n), \mathbf{out}(q_n))$ est un *effet observable*. Le mot $a_0.a_1 \dots a_{n-1}$ est un *séparateur*.

Exemple d'effets observables, cas déterministe

Dépliage de l'état q_0 du délai.



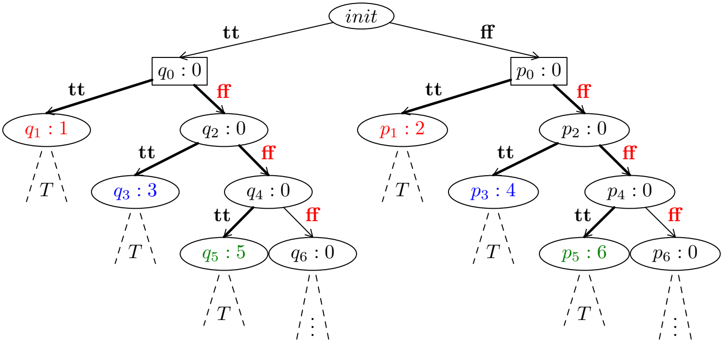
Tous les mots de longueur 2 sont des séparateurs de q_0 et q_1.
Exple :

$$\begin{array}{l|l} q_0 \xrightarrow{\mathbf{tt}} q_0 \xrightarrow{\mathbf{tt}} q_0 & \\ & \text{s.t. } \mathbf{out}(q_0) \neq \mathbf{out}(q_3). \\ q_1 \xrightarrow{\mathbf{tt}} q_2 \xrightarrow{\mathbf{tt}} q_3 & \end{array}$$

$\Rightarrow$ délai de séparabilité $= 2$

Exemple d'effets observables, cas déterministe - 2

Un dépliage où **ff*** ne contient pas de séparateurs.

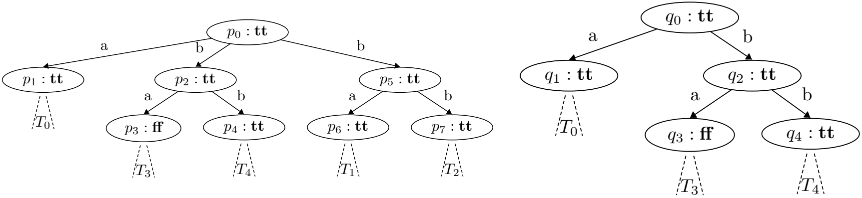


$$\left.\begin{array}{l} q_0 \xrightarrow{\mathbf{tt}} q_1 \\ p_0 \xrightarrow{\mathbf{tt}} p_1 \end{array}\right| \text{ s.t. } \mathbf{out}(q_1) \neq \mathbf{out}(p1).\text{Délai} = 1$$

Cas optimiste : séparateur = **tt**, délai = 1

Cas pessimiste : délai = ∞

Exemple d'effets observables, cas non-déterministe



$$\dfrac{\exists p_0 \xrightarrow{b} p_5, q_0 \xrightarrow{b} q_2 \mapsto \dfrac{\exists p_5 \xrightarrow{b} p_6, q_2 \xrightarrow{b} q_3 \mapsto \dfrac{\mathbf{tt} \neq \mathbf{ff}}{p_6 \not\sim q_3}\ \textsc{Base}}{p_5 \not\sim q_2}\ \textsc{Ind}}{p_0 \not\sim q_0}\ \textsc{Ind}$$

Le mot $b.a$ est un séparateur non-déterministe. Délai de séparabilité optimiste $= 2$, délai pessimiste $= \infty$

Des effets observables au délai de séparabilité

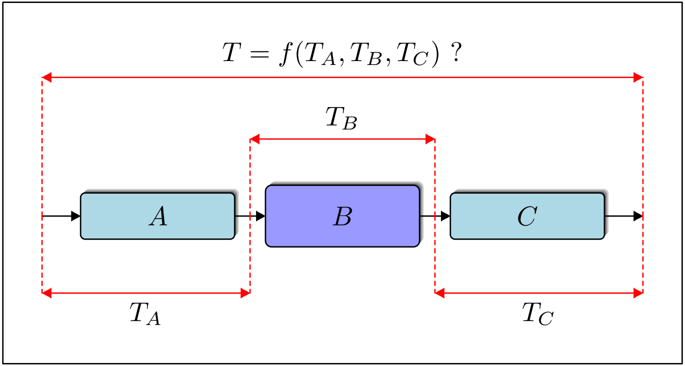
1. Réactivité d'un état q ($\equiv$ non-constance) $\leftrightarrow \exists$ **paire séparante** d'entrées $in_1 \neq in_2$ t.q. $q \xrightarrow{in_1} Q_1, q \xrightarrow{in_2} Q_2$ et ensemble Q_1 non équivalent à Q_2
2. Toute preuve de $q_i \nsim q_j$ produit au moins un **effet observable** généré par un mot d'entrée particulier appellé **séparateur**.

Délai de séparabilité

Existe en variantes pessimistes et optimistes. Correspond au nombre maximal (resp. minimal) de transitions nécessaires pour observer un effet observable.

Compositionalité

Systèmes temps-réels répartis = composition d'agents.

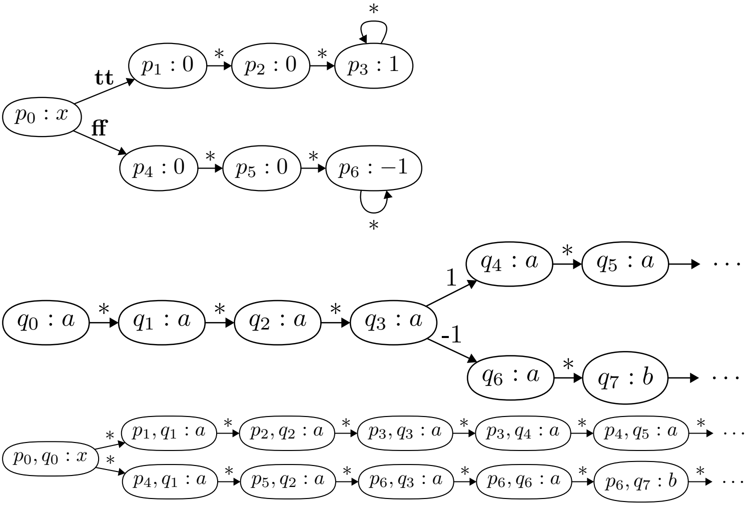


Peut-on calculer le délai de séparabilité global à partir de ceux de A, B et C ?

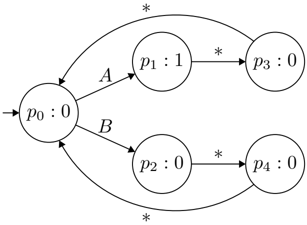
Composition séquentielle

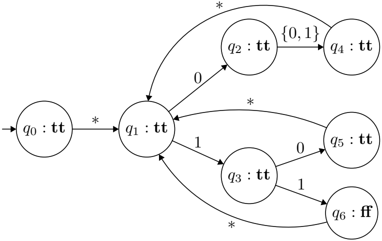
- Composition séquentielle = composition parallèle communicante.
- Espace d'état composé : si p état de la machine emettrice et q état de la machine réceptrice, état composé $= (p, q)$ avec $\mathbf{out}(p, q) = \mathbf{out}(q)$.
- Si $p \xrightarrow{a} p'$ est une transition de la machine emettrice et $q \xrightarrow{b} q'$ une transition de la machine réceptrice, la transition composée $(p, q) \xrightarrow{a} (p', q')$ existe ssi $b = \mathbf{out}(p)$.

Composition séquentielle - Exemple

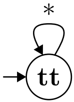


Non-compositionnalité





L'état q_6 devient inatteignable dans la composition, et q_2 et q_3 ne sont plus séparables. Résultat de la composition séquentielle :

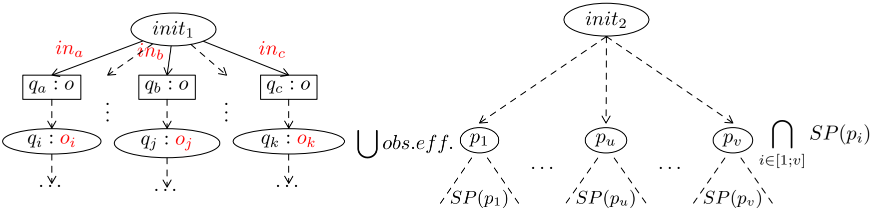


Pour calculer les effets observables composés, recherche exhaustive nécessaire.

Solution : choisir un sous-ensemble d'effets observables compositionnels

Approximer les effets observables

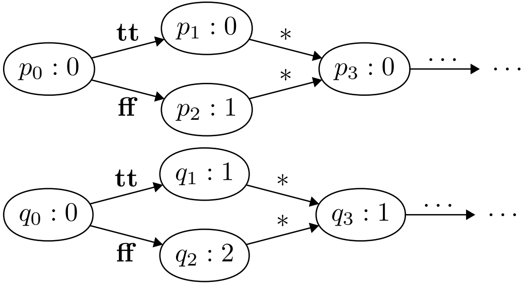
Idée centrale : la non-bisimilarité est une propriété en temps branchant. Se concentrer sur une sous-approximation en temps-linéaire.



Critère en temps linéaire : $init_2 \circ init_1$ réactif si $\bigcup obs.effects \subseteq \bigcap SP(q_i)$
Problème : calculer ces ensembles est complexe.

Déterminisme et séparabilité

Solution 2: restriction aux paires séparantes et effets observables présents pour tout mot d'entrée, i.e. "paires séparantes et effets observables déterministes"



contexte **tt**.**bool***, effet obs. $\emptyset.(0,1).(0,1)\ldots$

contexte **ff**.**bool***, effet obs. $\emptyset.(1,2).(0,1)\ldots$

effet obs. déterministe : $\emptyset.\emptyset.(0,1)\ldots$

Conclusion

- Délai de séparabilité défini en termes de preuves de non-bisimilarité
- En géneral, non-préservé par composition séquentielle
- Préservation dans le cas des effets obs. déterministes
- Application à la preuve du délai de bout-en-bout de systèmes de type OASIS

Perspectives :

- Idée applicable à tout modèle des systèmes réactifs (e.g. timed I/O automata)
- Liens avec la théorie de l'information. Le délai de séparabilité existe ssi au moins 1 bit d'information est transmis.